DMP:AFM
F.#2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH COMPUTER SERVERS HOSTED AT WEBZILLA AND SERVERS.COM	**TO BE FILED UNDER SEAL** **APPLICATION FOR SEARCH WARRANTS FOR INFORMATION IN POSSESSION OF PROVIDERS (COMPUTER SERVERS)** Case No. 18-mj-1019

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

I, EVELINA ASLANYAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for information on computer servers associated with certain IP addresses (the "Target IPs"), which is stored at premises owned, maintained, controlled, or operated by Webzilla Inc. ("Webzilla") and Servers.com Inc. ("Servers.com"), server providers respectively headquartered in Fort Lauderdale, Florida and Dallas, Texas (the "Providers"). The information to be searched is described in the following paragraphs and in Attachments A1 (with respect to Webzilla) and A2 (with respect to Servers.com).[1] This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Providers to disclose to the government copies of the information (including the content of

[1] Attachments A1 and A2 are identical except for the name of the provider. Attachments B1 and B2 are identical.

communications) further described in Section I of Attachments B1 and B2. Upon receipt of the information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I am responsible for conducting and assisting in investigations involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of the investigative file, and from reports of witnesses and other law enforcement officers involved in the investigation.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information further described in Attachments A1 and A2 for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and wire fraud conspiracy), further described in Attachments B1 and B2.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating an advertising fraud scheme known in the cybersecurity world as "Methbot," whose existence was first publicly reported on December 20, 2016 by researchers at a cybersecurity firm based in New York, New York (the "Cybersecurity Firm").[2]

7. The perpetrators of the Methbot scheme operated a purported digital advertising network called Mediamethane. (Advertising networks are entities specialized in placing digital ads with online publishers, so that they can be displayed to internet users browsing the publishers' websites.) Mediamethane had business arrangements with other advertising networks that enabled it to receive payment in return for placing advertisements with publishers on behalf of those advertising networks.

8. Evidence obtained in the course of the government's investigation shows that, rather than placing advertisements with real publishers, the perpetrators used servers that they controlled to create the illusion that a human internet user was viewing an online advertisement—when, in fact, a computer was loading the advertisement via an automated program—in order to fraudulently obtain a share of the resulting advertising revenue. In other words, the perpetrators did not arrange for the advertisements to appear on real webpages, but instead the perpetrators' servers browsed counterfeit versions of real webpages—typically

---

[2] FBI computer scientists have examined a sample of the underlying digital advertising signals that the Cybersecurity Firm relied on in issuing its report, and have confirmed that these signals are consistent with the fraud scheme described.

consisting of a blank box containing a space for a digital advertisement, with the purported publisher's name at the top.

9. In order to better disguise these servers as the computers of real internet users, the perpetrators submitted fraudulent entries to a global registry (the "WHOIS" database) that associates (a) domains and IP addresses with (b) name and address information, as well as other identifiers. The false information submitted by the perpetrators included the names of various major United States internet service providers—often distinctively misspelled—meant to convey the impression that the Target IPs belonged to human users of residential internet services.

10. Alexander Zhukov, a Russian national, identified himself as Mediamethane's CEO; the FBI's investigation has found that Boris Timokhin, also a Russian national, acted as the company's chief technical officer. Both individuals, along with three others, were charged by complaint on July 31, 2018 with conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349.

11. The scheme appears to have begun in or about September 2014, based on messages that the conspirators posted to a private discussion platform that they used to coordinate their activities. The scheme ended in or around December 2016, likely as a result of the Cybersecurity Firm's publication of its report.

A. The Cybsersecurity Firm Publishes a List of IP Addresses Linked to Methbot

12. Together with its December 2016 report, the Cybersecurity Firm published a list of approximately 600,000 IP addresses corresponding to computers that were fraudulently loading advertisements as part of the Methbot scheme. These IP addresses are the Target IPs. The government has obtained records regarding the Target IPs from Domaintools, an organization that continually archives data from the WHOIS database.

13. The dataset obtained from Domaintools (the "Domaintools Dataset"), viewed together with other evidence in this investigation, indicates that the Target IPs belonged to Zhukov and his coconspirators.

14. For example, as discussed above, the Domaintools Dataset shows that many of the Target IPs were associated in the WHOIS database with invented names meant to resemble those of United States internet service providers. These names included "ATOL Intertnet" and "AmOL wireless Net" (both apparently meant to resemble "[redacted] as well as "[redacted]," "[redacted]," "[redacted]," and "[redacted]." The FBI contacted six large United States internet service providers whose names were used or imitated in the Domaintools dataset, including [redacted] Each of the internet service providers stated that it had never controlled any of the Target IPs.

15. During the course of this investigation, the government obtained the contents of Zhukov's iCloud cloud storage account through a search warrant. Information from Apple indicates that an iPad, multiple iPhones, and multiple Apple desktop computers had access to the iCloud cloud storage account. The contents of Zhukov's iCloud account included a note dated September 18, 2015 that listed many of the fraudulent corporate names used to register the Target IPs. The list included [redacted] all of which were used to register the Target IPs, as shown in the Domaintools Dataset.

16. The Domaintools Dataset reflects that the fraudulent names listed in Zhukov's note were used to register certain of the Target IPs no later than March 2015.[3] For example, Domaintools recorded on March 31, 2015 that the IP address 181.214.168.0, which is one of the Target IPs, was registered as belonging to "[redacted]."

17. The government further obtained the contents of one of Boris Timokhin's email accounts. An FBI computer scientist searched Timokhin's emails for occurrences of the Target IPs, and found that approximately 15,500 unique Target IPs appeared in emails sent or received by Timokhin.

18. In addition, on April 24, 2016, Zhukov sent an email arranging to register 131,072 IP addresses using the name "[redacted]," which appears as a registered name for the Target IPs in the Domaintools Dataset.

B. The Target IPs Belong to Webzilla and Servers.com

19. The FBI has determined that the Methbot conspirators operated their scheme using servers at a datacenter in Dallas, Texas controlled by the server hosting companies Webzilla and Servers.com.

20. FBI agents have reviewed information from Routeviews.org ("Routeviews"), a publicly accessible service that tracks the path taken by packets of data in moving across the internet to and from specified servers. Data from Routeviews demonstrates that signals directed to the Target IPs traveled to servers operated by Servers.com, Inc. and WZ Communications Inc.

---

[3] Domaintools is not instantly updated when a WHOIS registration changes; rather, it searches for and records updated WHOIS data at periodic intervals. Thus, the fact that Domaintools records a particular WHOIS entry on a given date does not preclude the possibility that the WHOIS entry was created earlier than that date.

F#: 2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE: SEARCH WARRANT TO DROPBOX	TO BE FILED UNDER SEAL No. 17 MC 17M561

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Dropbox, an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the search warrant) of the existence of the attached search warrant until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving the targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Dropbox shall not disclose the existence of the attached search warrant, or this Order of the Court, to the listed subscriber or to any other person, unless and until otherwise authorized to do so by the Court, except that Dropbox may disclose the attached search warrant to attorneys for Dropbox for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

Dated: Brooklyn, New York
June 23, 2017

UNITED STATES MAGISTRATE JUDGE
Eastern District of New York

through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet and FTP connections, showing the dates and times of the connections, the method of connecting, and the IP addresses of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

27. The servers use those files, software code, databases and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files. Server providers frequently allow their customers to store collections of data in databases. Software running on the server maintains those databases; two common such programs are named MySQL and PostgreSQL, although those are not the only ones.

28. Server providers sometimes provide their customers with email accounts; contents of those accounts are also stored on the company's servers.

29. In some cases, a subscriber or user will communicate direct with a server provider about issues relating to a website or account, such as technical problems, billing inquiries or complaints from other users. Server providers typically retain records about such communications, including records of contacts between the user and the company's support

services, as well as records of any actions taken by the company or user as a result of the communications.

CONCLUSION

30. I anticipate executing these warrants under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require the Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachments B1 and B2. Upon receipt of the information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

31. Based on the foregoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

33. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding the Providers not to notify any person (including the subscribers and customers of the servers listed in the warrants) of the existence of

the warrants for one year from the date the warrants are signed, except that the Providers may share a copy of the warrant with their respective attorneys for the purpose of obtaining legal advice.

Respectfully submitted,

EVELINA ASLANYAN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 25, 2018

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A1

Property To Be Searched

This warrant applies to information associated with the IP addresses within the ranges listed below (the "Target IPs") that correspond to servers hosted at Webzilla, Inc. (the "Provider"), an Internet service provider headquartered in Fort Lauderdale, Florida.

45.33.224.0 - 45.33.239.255
45.43.128.0 - 45.43.141.255
45.43.144.0 - 45.43.191.255
64.137.0.0 - 64.137.27.255
64.137.30.0 - 64.137.127.255
104.143.224.0 - 104.143.255.255
104.222.160.0 - 104.222.191.255
104.233.0.0 - 104.233.63.255
104.238.0.0 - 104.238.31.255
104.239.0.0 - 104.239.31.255
104.239.32.0 - 104.239.57.255
104.239.60.0 - 104.239.127.255
104.243.192.0 - 104.243.207.255
104.248.0.0 - 104.249.63.255
104.250.192.0 - 104.250.223.255
160.184.0.0 - 160.184.255.255
161.8.128.0 - 161.8.255.255
165.52.0.0 - 165.55.255.255
168.211.0.0 - 168.211.255.255
179.61.129.0 - 179.61.129.255
179.61.137.0 - 179.61.137.255
179.61.196.0 - 179.61.196.255
179.61.202.0 - 179.61.202.255
179.61.208.0 - 179.61.208.255
179.61.216.0 - 179.61.216.255
179.61.218.0 - 179.61.219.255
179.61.229.0 - 179.61.229.255
179.61.230.0 - 179.61.231.255
179.61.233.0 - 179.61.235.255
179.61.237.0 - 179.61.237.255
179.61.239.0 - 179.61.239.255
179.61.242.0 - 179.61.242.255
181.41.199.0 - 181.41.200.255
181.41.202.0 - 181.41.202.255
181.41.204.0 - 181.41.204.255
181.41.206.0 - 181.41.208.255
181.41.213.0 - 181.41.213.255
181.41.215.0 - 181.41.216.255
181.41.218.0 - 181.41.218.255
181.214.5.0 - 181.214.5.255
181.214.7.0 - 181.214.7.255
181.214.9.0 - 181.214.9.255
181.214.11.0 - 181.214.11.255
181.214.13.0 - 181.214.13.255
181.214.15.0 - 181.214.15.255
181.214.17.0 - 181.214.17.255
181.214.19.0 - 181.214.19.255
181.214.21.0 - 181.214.21.255
181.214.23.0 - 181.214.23.255
181.214.25.0 - 181.214.25.255
181.214.27.0 - 181.214.27.255
181.214.29.0 - 181.214.29.255
181.214.31.0 - 181.214.31.255
181.214.39.0 - 181.214.39.255
181.214.41.0 - 181.214.41.255
181.214.43.0 - 181.214.43.255
181.214.45.0 - 181.214.45.255
181.214.47.0 - 181.214.47.255
181.214.49.0 - 181.214.49.255
181.214.57.0 - 181.214.57.255
181.214.71.0 - 181.214.89.255
181.214.94.0 - 181.214.127.255
181.214.160.0 - 181.214.173.255
181.214.175.0 - 181.214.175.255
181.214.176.0 - 181.214.203.255
181.214.214.0 - 181.214.243.255
181.215.5.0 - 181.215.5.255
181.215.7.0 - 181.215.7.255

181.215.9.0 - 181.215.9.255
181.215.11.0 - 181.215.11.255
181.215.13.0 - 181.215.13.255
181.215.15.0 - 181.215.15.255
181.215.17.0 - 181.215.17.255
181.215.19.0 - 181.215.19.255
181.215.21.0 - 181.215.21.255
181.215.23.0 - 181.215.23.255
181.215.25.0 - 181.215.25.255
181.215.27.0 - 181.215.27.255
181.215.29.0 - 181.215.29.255
181.215.31.0 - 181.215.31.255
181.215.33.0 - 181.215.33.255
181.215.35.0 - 181.215.35.255
181.215.37.0 - 181.215.37.255
181.215.39.0 - 181.215.39.255
181.215.41.0 - 181.215.41.255
181.215.43.0 - 181.215.43.255
181.215.45.0 - 181.215.45.255
181.215.47.0 - 181.215.47.255
181.215.50.0 - 181.215.63.255
181.215.64.0 - 181.215.87.255
188.42.0.0 - 188.42.7.255
191.96.0.0 - 191.96.0.255
191.96.16.0 - 191.96.16.255
191.96.18.0 - 191.96.18.255
191.96.21.0 - 191.96.21.255
191.96.23.0 - 191.96.23.255
191.96.29.0 - 191.96.30.255
191.96.39.0 - 191.96.39.255
191.96.40.0 - 191.96.41.255
191.96.43.0 - 191.96.43.255
191.96.44.0 - 191.96.47.255
191.96.50.0 - 191.96.62.255
191.96.69.0 - 191.96.69.255
191.96.70.0 - 191.96.74.255
191.96.76.0 - 191.96.92.255
191.96.94.0 - 191.96.94.255
191.96.96.0 - 191.96.97.255
191.96.108.0 - 191.96.110.255
191.96.113.0 - 191.96.114.255
191.96.116.0 - 191.96.117.255
191.96.119.0 - 191.96.122.255
191.96.124.0 - 191.96.127.255
191.96.133.0 - 191.96.134.255
191.96.138.0 - 191.96.138.255
191.96.140.0 - 191.96.140.255
191.96.145.0 - 191.96.145.255
191.96.148.0 - 191.96.148.255
191.96.150.0 - 191.96.150.255
191.96.152.0 - 191.96.164.255
191.96.168.0 - 191.96.168.255
191.96.170.0 - 191.96.170.255
191.96.172.0 - 191.96.172.255
191.96.174.0 - 191.96.174.255
191.96.177.0 - 191.96.179.255
191.96.182.0 - 191.96.182.255
191.96.185.0 - 191.96.187.255
191.96.189.0 - 191.96.190.255
191.96.193.0 - 191.96.193.255
191.96.194.0 - 191.96.194.255
191.96.196.0 - 191.96.201.255
191.96.203.0 - 191.96.203.255
191.96.210.0 - 191.96.210.255
191.96.212.0 - 191.96.214.255
191.96.221.0 - 191.96.223.255
191.96.226.0 - 191.96.227.255
191.96.232.0 - 191.96.232.255
191.96.234.0 - 191.96.237.255
191.96.239.0 - 191.96.239.255
191.96.244.0 - 191.96.244.255
191.96.246.0 - 191.96.246.255
191.101.25.0 - 191.101.25.255
191.101.36.0 - 191.101.39.255
191.101.40.0 - 191.101.47.255
191.101.128.0 - 191.101.134.255
191.101.146.0 - 191.101.147.255
191.101.148.0 - 191.101.149.255
191.101.176.0 - 191.101.177.255
191.101.182.0 - 191.101.182.255
191.101.184.0 - 191.101.189.255
191.101.192.0 - 191.101.197.255
191.101.204.0 - 191.101.207.255
191.101.216.0 - 191.101.220.255
191.101.222.0 - 191.101.223.255
196.62.0.0 - 196.62.255.255
204.52.96.0 - 204.52.117.255
204.52.120.0 - 204.52.121.255
204.52.122.0 - 204.52.122.255
204.52.124.0 - 204.52.127.255

206.124.104.0 - 206.124.111.255
209.192.128.0 - 209.192.159.255
216.173.64.0 - 216.173.127.255

ATTACHMENT B1

Particular Things To Be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the period from January 1, 2015 to January 1, 2017:

a. All records and other information pertaining to the Target IPs, including all files, databases, IP logs and database records stored by the Provider in relation to the Target IPs;

b. All information in the possession of the Provider that might identify the subscriber(s) and user(s) related to the Target IPs, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service utilized by the subscriber(s) and user(s) of the Target IPs;

d. All records pertaining to communications between the Provider and any person regarding the Target IPs, including contacts with support services and records of actions taken;

e. All records pertaining to the physical location of the servers used to host the Target IPs;

f. All files, databases and other content information pertaining to the Target IPs stored on behalf of its subscriber(s) and user(s), including:

1. All volatile memory used by virtualized and physical computers;
2. Programming code used to serve or process requests from email clients;
3. SSH, FTP or similar logs showing connections related to the Target IPs, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;
4. MySQL, PostgreSQL, or other databases related to website(s);
5. Email accounts and the contents thereof, associated with the servers; and
6. A forensic image of the servers associated with the Target IPs, including any historic images;

g. All records and information, including passwords, encryption keys, and other access devices, that may be necessary to access the information associated with the Target IPs.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the servers associated with the Target IPs, their co - conspirators, their associates and others with whom they communicated, including information pertaining to the following matters:

a. Committing, conspiring or attempting to commit wire fraud;

b. Evidence indicating how and when the servers associated with the Target IPs were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the servers' users;

c. Evidence indicating the state of mind of the user(s) of the servers associated with the Target IPs, as it relates to the crimes under investigation;

d. The identity of the person(s) who leased, used, or controlled the servers associated with the Target IPs, including records that help reveal the whereabouts of such person(s).

e. The identity of the persons(s) and computer(s) that communicated with the servers associated with the Target IPs in relation to wire fraud and conspiracy or attempt to commit wire fraud, including records that help reveal their whereabouts.

ATTACHMENT A2

Property To Be Searched

This warrant applies to information associated with the IP addresses within the ranges listed below (the "Target IPs") that correspond to servers hosted at Servers.com Inc. (the "Provider"), an Internet service provider headquartered in Dallas, Texas.

45.33.224.0 - 45.33.239.255
45.43.128.0 - 45.43.141.255
45.43.144.0 - 45.43.191.255
64.137.0.0 - 64.137.27.255
64.137.30.0 - 64.137.127.255
104.143.224.0 - 104.143.255.255
104.222.160.0 - 104.222.191.255
104.233.0.0 - 104.233.63.255
104.238.0.0 - 104.238.31.255
104.239.0.0 - 104.239.31.255
104.239.32.0 - 104.239.57.255
104.239.60.0 - 104.239.127.255
104.243.192.0 - 104.243.207.255
104.248.0.0 - 104.249.63.255
104.250.192.0 - 104.250.223.255
160.184.0.0 - 160.184.255.255
161.8.128.0 - 161.8.255.255
165.52.0.0 - 165.55.255.255
168.211.0.0 - 168.211.255.255
179.61.129.0 - 179.61.129.255
179.61.137.0 - 179.61.137.255
179.61.196.0 - 179.61.196.255
179.61.202.0 - 179.61.202.255
179.61.208.0 - 179.61.208.255
179.61.216.0 - 179.61.216.255
179.61.218.0 - 179.61.219.255
179.61.229.0 - 179.61.229.255
179.61.230.0 - 179.61.231.255
179.61.233.0 - 179.61.235.255
179.61.237.0 - 179.61.237.255
179.61.239.0 - 179.61.239.255
179.61.242.0 - 179.61.242.255
181.41.199.0 - 181.41.200.255
181.41.202.0 - 181.41.202.255
181.41.204.0 - 181.41.204.255
181.41.206.0 - 181.41.208.255
181.41.213.0 - 181.41.213.255
181.41.215.0 - 181.41.216.255
181.41.218.0 - 181.41.218.255
181.214.5.0 - 181.214.5.255
181.214.7.0 - 181.214.7.255
181.214.9.0 - 181.214.9.255
181.214.11.0 - 181.214.11.255
181.214.13.0 - 181.214.13.255
181.214.15.0 - 181.214.15.255
181.214.17.0 - 181.214.17.255
181.214.19.0 - 181.214.19.255
181.214.21.0 - 181.214.21.255
181.214.23.0 - 181.214.23.255
181.214.25.0 - 181.214.25.255
181.214.27.0 - 181.214.27.255
181.214.29.0 - 181.214.29.255
181.214.31.0 - 181.214.31.255
181.214.39.0 - 181.214.39.255
181.214.41.0 - 181.214.41.255
181.214.43.0 - 181.214.43.255
181.214.45.0 - 181.214.45.255
181.214.47.0 - 181.214.47.255
181.214.49.0 - 181.214.49.255
181.214.57.0 - 181.214.57.255
181.214.71.0 - 181.214.89.255
181.214.94.0 - 181.214.127.255
181.214.160.0 - 181.214.173.255
181.214.175.0 - 181.214.175.255
181.214.176.0 - 181.214.203.255
181.214.214.0 - 181.214.243.255

181.215.5.0 - 181.215.5.255
181.215.7.0 - 181.215.7.255
181.215.9.0 - 181.215.9.255
181.215.11.0 - 181.215.11.255
181.215.13.0 - 181.215.13.255
181.215.15.0 - 181.215.15.255
181.215.17.0 - 181.215.17.255
181.215.19.0 - 181.215.19.255
181.215.21.0 - 181.215.21.255
181.215.23.0 - 181.215.23.255
181.215.25.0 - 181.215.25.255
181.215.27.0 - 181.215.27.255
181.215.29.0 - 181.215.29.255
181.215.31.0 - 181.215.31.255
181.215.33.0 - 181.215.33.255
181.215.35.0 - 181.215.35.255
181.215.37.0 - 181.215.37.255
181.215.39.0 - 181.215.39.255
181.215.41.0 - 181.215.41.255
181.215.43.0 - 181.215.43.255
181.215.45.0 - 181.215.45.255
181.215.47.0 - 181.215.47.255
181.215.50.0 - 181.215.63.255
181.215.64.0 - 181.215.87.255
188.42.0.0 - 188.42.7.255
191.96.0.0 - 191.96.0.255
191.96.16.0 - 191.96.16.255
191.96.18.0 - 191.96.18.255
191.96.21.0 - 191.96.21.255
191.96.23.0 - 191.96.23.255
191.96.29.0 - 191.96.30.255
191.96.39.0 - 191.96.39.255
191.96.40.0 - 191.96.41.255
191.96.43.0 - 191.96.43.255
191.96.44.0 - 191.96.47.255
191.96.50.0 - 191.96.62.255
191.96.69.0 - 191.96.69.255
191.96.70.0 - 191.96.74.255
191.96.76.0 - 191.96.92.255
191.96.94.0 - 191.96.94.255
191.96.96.0 - 191.96.97.255
191.96.108.0 - 191.96.110.255
191.96.113.0 - 191.96.114.255
191.96.116.0 - 191.96.117.255
191.96.119.0 - 191.96.122.255
191.96.124.0 - 191.96.127.255
191.96.133.0 - 191.96.134.255
191.96.138.0 - 191.96.138.255
191.96.140.0 - 191.96.140.255
191.96.145.0 - 191.96.145.255
191.96.148.0 - 191.96.148.255
191.96.150.0 - 191.96.150.255
191.96.152.0 - 191.96.164.255
191.96.168.0 - 191.96.168.255
191.96.170.0 - 191.96.170.255
191.96.172.0 - 191.96.172.255
191.96.174.0 - 191.96.174.255
191.96.177.0 - 191.96.179.255
191.96.182.0 - 191.96.182.255
191.96.185.0 - 191.96.187.255
191.96.189.0 - 191.96.190.255
191.96.193.0 - 191.96.193.255
191.96.194.0 - 191.96.194.255
191.96.196.0 - 191.96.201.255
191.96.203.0 - 191.96.203.255
191.96.210.0 - 191.96.210.255
191.96.212.0 - 191.96.214.255
191.96.221.0 - 191.96.223.255
191.96.226.0 - 191.96.227.255
191.96.232.0 - 191.96.232.255
191.96.234.0 - 191.96.237.255
191.96.239.0 - 191.96.239.255
191.96.244.0 - 191.96.244.255
191.96.246.0 - 191.96.246.255
191.101.25.0 - 191.101.25.255
191.101.36.0 - 191.101.39.255
191.101.40.0 - 191.101.47.255
191.101.128.0 - 191.101.134.255
191.101.146.0 - 191.101.147.255
191.101.148.0 - 191.101.149.255
191.101.176.0 - 191.101.177.255
191.101.182.0 - 191.101.182.255
191.101.184.0 - 191.101.189.255
191.101.192.0 - 191.101.197.255
191.101.204.0 - 191.101.207.255
191.101.216.0 - 191.101.220.255
191.101.222.0 - 191.101.223.255
196.62.0.0 - 196.62.255.255
204.52.96.0 - 204.52.117.255
204.52.120.0 - 204.52.121.255

204.52.122.0 - 204.52.122.255
204.52.124.0 - 204.52.127.255
206.124.104.0 - 206.124.111.255
209.192.128.0 - 209.192.159.255
216.173.64.0 - 216.173.127.255

ATTACHMENT B2

Particular Things To Be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A2 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the period from January 1, 2015 to January 1, 2017:

a. All records and other information pertaining to the Target IPs, including all files, databases, IP logs and database records stored by the Provider in relation to the Target IPs;

b. All information in the possession of the Provider that might identify the subscriber(s) and user(s) related to the Target IPs, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service utilized by the subscriber(s) and user(s) of the Target IPs;

d. All records pertaining to communications between the Provider and any person regarding the Target IPs, including contacts with support services and records of actions taken;

e. All records pertaining to the physical location of the servers used to host the Target IPs;

f. All files, databases and other content information pertaining to the Target IPs stored on behalf of its subscriber(s) and user(s), including:

7. All volatile memory used by virtualized and physical computers;
8. Programming code used to serve or process requests from email clients;
9. SSH, FTP or similar logs showing connections related to the Target IPs, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;
10. MySQL, PostgreSQL, or other databases related to website(s);
11. Email accounts and the contents thereof, associated with the servers; and
12. A forensic image of the servers associated with the Target IPs, including any historic images;

g. All records and information, including passwords, encryption keys, and other access devices, that may be necessary to access the information associated with the Target IPs.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the servers associated with the Target IPs, their co - conspirators, their associates and others with whom they communicated, including information pertaining to the following matters:

a. Committing, conspiring or attempting to commit wire fraud;

b. Evidence indicating how and when the servers associated with the Target IPs were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the servers' users;

c. Evidence indicating the state of mind of the user(s) of the servers associated with the Target IPs, as it relates to the crimes under investigation;

d. The identity of the person(s) who leased, used, or controlled the servers associated with the Target IPs, including records that help reveal the whereabouts of such person(s).

e. The identity of the persons(s) and computer(s) that communicated with the servers associated with the Target IPs in relation to wire fraud and conspiracy or attempt to commit wire fraud, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information Associated with Computer Servers Hosted at Servers.com	)	Case No. 18-mj-1019

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2018 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 10/25/18 @ 1:23 p.m.

Judge's signature

City and state: Brooklyn, New York

Hon. Ramon E. Reyes, Jr. U.S.M.J.
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with the IP addresses within the ranges listed below (the "Target IPs") that correspond to servers hosted at Servers.com Inc. (the "Provider"), an Internet service provider headquartered in Dallas, Texas.

45.33.224.0 - 45.33.239.255
45.43.128.0 - 45.43.141.255
45.43.144.0 - 45.43.191.255
64.137.0.0 - 64.137.27.255
64.137.30.0 - 64.137.127.255
104.143.224.0 - 104.143.255.255
104.222.160.0 - 104.222.191.255
104.233.0.0 - 104.233.63.255
104.238.0.0 - 104.238.31.255
104.239.0.0 - 104.239.31.255
104.239.32.0 - 104.239.57.255
104.239.60.0 - 104.239.127.255
104.243.192.0 - 104.243.207.255
104.248.0.0 - 104.249.63.255
104.250.192.0 - 104.250.223.255
160.184.0.0 - 160.184.255.255
161.8.128.0 - 161.8.255.255
165.52.0.0 - 165.55.255.255
168.211.0.0 - 168.211.255.255
179.61.129.0 - 179.61.129.255
179.61.137.0 - 179.61.137.255
179.61.196.0 - 179.61.196.255
179.61.202.0 - 179.61.202.255
179.61.208.0 - 179.61.208.255
179.61.216.0 - 179.61.216.255
179.61.218.0 - 179.61.219.255
179.61.229.0 - 179.61.229.255
179.61.230.0 - 179.61.231.255
179.61.233.0 - 179.61.235.255
179.61.237.0 - 179.61.237.255
179.61.239.0 - 179.61.239.255
179.61.242.0 - 179.61.242.255
181.41.199.0 - 181.41.200.255
181.41.202.0 - 181.41.202.255
181.41.204.0 - 181.41.204.255
181.41.206.0 - 181.41.208.255
181.41.213.0 - 181.41.213.255
181.41.215.0 - 181.41.216.255
181.41.218.0 - 181.41.218.255
181.214.5.0 - 181.214.5.255
181.214.7.0 - 181.214.7.255
181.214.9.0 - 181.214.9.255
181.214.11.0 - 181.214.11.255
181.214.13.0 - 181.214.13.255
181.214.15.0 - 181.214.15.255
181.214.17.0 - 181.214.17.255
181.214.19.0 - 181.214.19.255
181.214.21.0 - 181.214.21.255
181.214.23.0 - 181.214.23.255
181.214.25.0 - 181.214.25.255
181.214.27.0 - 181.214.27.255
181.214.29.0 - 181.214.29.255
181.214.31.0 - 181.214.31.255
181.214.39.0 - 181.214.39.255
181.214.41.0 - 181.214.41.255
181.214.43.0 - 181.214.43.255
181.214.45.0 - 181.214.45.255
181.214.47.0 - 181.214.47.255
181.214.49.0 - 181.214.49.255
181.214.57.0 - 181.214.57.255
181.214.71.0 - 181.214.89.255
181.214.94.0 - 181.214.127.255
181.214.160.0 - 181.214.173.255
181.214.175.0 - 181.214.175.255
181.214.176.0 - 181.214.203.255
181.214.214.0 - 181.214.243.255
181.215.5.0 - 181.215.5.255
181.215.7.0 - 181.215.7.255

181.215.9.0 - 181.215.9.255
181.215.11.0 - 181.215.11.255
181.215.13.0 - 181.215.13.255
181.215.15.0 - 181.215.15.255
181.215.17.0 - 181.215.17.255
181.215.19.0 - 181.215.19.255
181.215.21.0 - 181.215.21.255
181.215.23.0 - 181.215.23.255
181.215.25.0 - 181.215.25.255
181.215.27.0 - 181.215.27.255
181.215.29.0 - 181.215.29.255
181.215.31.0 - 181.215.31.255
181.215.33.0 - 181.215.33.255
181.215.35.0 - 181.215.35.255
181.215.37.0 - 181.215.37.255
181.215.39.0 - 181.215.39.255
181.215.41.0 - 181.215.41.255
181.215.43.0 - 181.215.43.255
181.215.45.0 - 181.215.45.255
181.215.47.0 - 181.215.47.255
181.215.50.0 - 181.215.63.255
181.215.64.0 - 181.215.87.255
188.42.0.0 - 188.42.7.255
191.96.0.0 - 191.96.0.255
191.96.16.0 - 191.96.16.255
191.96.18.0 - 191.96.18.255
191.96.21.0 - 191.96.21.255
191.96.23.0 - 191.96.23.255
191.96.29.0 - 191.96.30.255
191.96.39.0 - 191.96.39.255
191.96.40.0 - 191.96.41.255
191.96.43.0 - 191.96.43.255
191.96.44.0 - 191.96.47.255
191.96.50.0 - 191.96.62.255
191.96.69.0 - 191.96.69.255
191.96.70.0 - 191.96.74.255
191.96.76.0 - 191.96.92.255
191.96.94.0 - 191.96.94.255
191.96.96.0 - 191.96.97.255
191.96.108.0 - 191.96.110.255
191.96.113.0 - 191.96.114.255
191.96.116.0 - 191.96.117.255
191.96.119.0 - 191.96.122.255
191.96.124.0 - 191.96.127.255
191.96.133.0 - 191.96.134.255
191.96.138.0 - 191.96.138.255
191.96.140.0 - 191.96.140.255
191.96.145.0 - 191.96.145.255
191.96.148.0 - 191.96.148.255
191.96.150.0 - 191.96.150.255
191.96.152.0 - 191.96.164.255
191.96.168.0 - 191.96.168.255
191.96.170.0 - 191.96.170.255
191.96.172.0 - 191.96.172.255
191.96.174.0 - 191.96.174.255
191.96.177.0 - 191.96.179.255
191.96.182.0 - 191.96.182.255
191.96.185.0 - 191.96.187.255
191.96.189.0 - 191.96.190.255
191.96.193.0 - 191.96.193.255
191.96.194.0 - 191.96.194.255
191.96.196.0 - 191.96.201.255
191.96.203.0 - 191.96.203.255
191.96.210.0 - 191.96.210.255
191.96.212.0 - 191.96.214.255
191.96.221.0 - 191.96.223.255
191.96.226.0 - 191.96.227.255
191.96.232.0 - 191.96.232.255
191.96.234.0 - 191.96.237.255
191.96.239.0 - 191.96.239.255
191.96.244.0 - 191.96.244.255
191.96.246.0 - 191.96.246.255
191.101.25.0 - 191.101.25.255
191.101.36.0 - 191.101.39.255
191.101.40.0 - 191.101.47.255
191.101.128.0 - 191.101.134.255
191.101.146.0 - 191.101.147.255
191.101.148.0 - 191.101.149.255
191.101.176.0 - 191.101.177.255
191.101.182.0 - 191.101.182.255
191.101.184.0 - 191.101.189.255
191.101.192.0 - 191.101.197.255
191.101.204.0 - 191.101.207.255
191.101.216.0 - 191.101.220.255
191.101.222.0 - 191.101.223.255
196.62.0.0 - 196.62.255.255
204.52.96.0 - 204.52.117.255
204.52.120.0 - 204.52.121.255
204.52.122.0 - 204.52.122.255
204.52.124.0 - 204.52.127.255
206.124.104.0 - 206.124.111.255
209.192.128.0 - 209.192.159.255

216.173.64.0 - 216.173.127.255

ATTACHMENT B

Particular Things To Be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the period from January 1, 2015 to January 1, 2017:

a. All records and other information pertaining to the Target IPs, including all files, databases, IP logs and database records stored by the Provider in relation to the Target IPs;

b. All information in the possession of the Provider that might identify the subscriber(s) and user(s) related to the Target IPs, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service utilized by the subscriber(s) and user(s) of the Target IPs;

d. All records pertaining to communications between the Provider and any person regarding the Target IPs, including contacts with support services and records of actions taken;

e. All records pertaining to the physical location of the servers used to host the Target IPs;

f. All files, databases and other content information pertaining to the Target IPs stored on behalf of its subscriber(s) and user(s), including:

1. All volatile memory used by virtualized and physical computers;
2. Programming code used to serve or process requests from email clients;
3. SSH, FTP or similar logs showing connections related to the Target IPs, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;
4. MySQL, PostgreSQL, or other databases related to website(s);
5. Email accounts and the contents thereof, associated with the servers; and
6. A forensic image of the servers associated with the Target IPs, including any historic images;

g. All records and information, including passwords, encryption keys, and other access devices, that may be necessary to access the information associated with the Target IPs.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the servers associated with the Target IPs, their co - conspirators, their associates and others with whom they communicated, including information pertaining to the following matters:

a. Committing, conspiring or attempting to commit wire fraud;

b. Evidence indicating how and when the servers associated with the Target IPs were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the servers' users;

c. Evidence indicating the state of mind of the user(s) of the servers associated with the Target IPs, as it relates to the crimes under investigation;

d. The identity of the person(s) who leased, used, or controlled the servers associated with the Target IPs, including records that help reveal the whereabouts of such person(s).

e. The identity of the persons(s) and computer(s) that communicated with the servers associated with the Target IPs in relation to wire fraud and conspiracy or attempt to commit wire fraud, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information Associated with Computer Servers Hosted at Webzilla	)	Case No. 18-mj-1019

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2018 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 10/25/18 @ 1:23 p.m.

Judge's signature

City and state: Brooklyn, New York

Hon. Ramon E. Reyes, Jr. U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 18-mj-1019	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with the IP addresses within the ranges listed below (the "Target IPs") that correspond to servers hosted at Webzilla, Inc. (the "Provider"), an Internet service provider headquartered in Fort Lauderdale, Florida.

45.33.224.0 - 45.33.239.255
45.43.128.0 - 45.43.141.255
45.43.144.0 - 45.43.191.255
64.137.0.0 - 64.137.27.255
64.137.30.0 - 64.137.127.255
104.143.224.0 - 104.143.255.255
104.222.160.0 - 104.222.191.255
104.233.0.0 - 104.233.63.255
104.238.0.0 - 104.238.31.255
104.239.0.0 - 104.239.31.255
104.239.32.0 - 104.239.57.255
104.239.60.0 - 104.239.127.255
104.243.192.0 - 104.243.207.255
104.248.0.0 - 104.249.63.255
104.250.192.0 - 104.250.223.255
160.184.0.0 - 160.184.255.255
161.8.128.0 - 161.8.255.255
165.52.0.0 - 165.55.255.255
168.211.0.0 - 168.211.255.255
179.61.129.0 - 179.61.129.255
179.61.137.0 - 179.61.137.255
179.61.196.0 - 179.61.196.255
179.61.202.0 - 179.61.202.255
179.61.208.0 - 179.61.208.255
179.61.216.0 - 179.61.216.255
179.61.218.0 - 179.61.219.255
179.61.229.0 - 179.61.229.255
179.61.230.0 - 179.61.231.255
179.61.233.0 - 179.61.235.255
179.61.237.0 - 179.61.237.255
179.61.239.0 - 179.61.239.255
179.61.242.0 - 179.61.242.255
181.41.199.0 - 181.41.200.255
181.41.202.0 - 181.41.202.255
181.41.204.0 - 181.41.204.255
181.41.206.0 - 181.41.208.255
181.41.213.0 - 181.41.213.255
181.41.215.0 - 181.41.216.255
181.41.218.0 - 181.41.218.255
181.214.5.0 - 181.214.5.255
181.214.7.0 - 181.214.7.255
181.214.9.0 - 181.214.9.255
181.214.11.0 - 181.214.11.255
181.214.13.0 - 181.214.13.255
181.214.15.0 - 181.214.15.255
181.214.17.0 - 181.214.17.255
181.214.19.0 - 181.214.19.255
181.214.21.0 - 181.214.21.255
181.214.23.0 - 181.214.23.255
181.214.25.0 - 181.214.25.255
181.214.27.0 - 181.214.27.255
181.214.29.0 - 181.214.29.255
181.214.31.0 - 181.214.31.255
181.214.39.0 - 181.214.39.255
181.214.41.0 - 181.214.41.255
181.214.43.0 - 181.214.43.255
181.214.45.0 - 181.214.45.255
181.214.47.0 - 181.214.47.255
181.214.49.0 - 181.214.49.255
181.214.57.0 - 181.214.57.255
181.214.71.0 - 181.214.89.255
181.214.94.0 - 181.214.127.255
181.214.160.0 - 181.214.173.255
181.214.175.0 - 181.214.175.255
181.214.176.0 - 181.214.203.255
181.214.214.0 - 181.214.243.255
181.215.5.0 - 181.215.5.255
181.215.7.0 - 181.215.7.255

181.215.9.0 - 181.215.9.255
181.215.11.0 - 181.215.11.255
181.215.13.0 - 181.215.13.255
181.215.15.0 - 181.215.15.255
181.215.17.0 - 181.215.17.255
181.215.19.0 - 181.215.19.255
181.215.21.0 - 181.215.21.255
181.215.23.0 - 181.215.23.255
181.215.25.0 - 181.215.25.255
181.215.27.0 - 181.215.27.255
181.215.29.0 - 181.215.29.255
181.215.31.0 - 181.215.31.255
181.215.33.0 - 181.215.33.255
181.215.35.0 - 181.215.35.255
181.215.37.0 - 181.215.37.255
181.215.39.0 - 181.215.39.255
181.215.41.0 - 181.215.41.255
181.215.43.0 - 181.215.43.255
181.215.45.0 - 181.215.45.255
181.215.47.0 - 181.215.47.255
181.215.50.0 - 181.215.63.255
181.215.64.0 - 181.215.87.255
188.42.0.0 - 188.42.7.255
191.96.0.0 - 191.96.0.255
191.96.16.0 - 191.96.16.255
191.96.18.0 - 191.96.18.255
191.96.21.0 - 191.96.21.255
191.96.23.0 - 191.96.23.255
191.96.29.0 - 191.96.30.255
191.96.39.0 - 191.96.39.255
191.96.40.0 - 191.96.41.255
191.96.43.0 - 191.96.43.255
191.96.44.0 - 191.96.47.255
191.96.50.0 - 191.96.62.255
191.96.69.0 - 191.96.69.255
191.96.70.0 - 191.96.74.255
191.96.76.0 - 191.96.92.255
191.96.94.0 - 191.96.94.255
191.96.96.0 - 191.96.97.255
191.96.108.0 - 191.96.110.255
191.96.113.0 - 191.96.114.255
191.96.116.0 - 191.96.117.255
191.96.119.0 - 191.96.122.255
191.96.124.0 - 191.96.127.255
191.96.133.0 - 191.96.134.255
191.96.138.0 - 191.96.138.255
191.96.140.0 - 191.96.140.255
191.96.145.0 - 191.96.145.255
191.96.148.0 - 191.96.148.255
191.96.150.0 - 191.96.150.255
191.96.152.0 - 191.96.164.255
191.96.168.0 - 191.96.168.255
191.96.170.0 - 191.96.170.255
191.96.172.0 - 191.96.172.255
191.96.174.0 - 191.96.174.255
191.96.177.0 - 191.96.179.255
191.96.182.0 - 191.96.182.255
191.96.185.0 - 191.96.187.255
191.96.189.0 - 191.96.190.255
191.96.193.0 - 191.96.193.255
191.96.194.0 - 191.96.194.255
191.96.196.0 - 191.96.201.255
191.96.203.0 - 191.96.203.255
191.96.210.0 - 191.96.210.255
191.96.212.0 - 191.96.214.255
191.96.221.0 - 191.96.223.255
191.96.226.0 - 191.96.227.255
191.96.232.0 - 191.96.232.255
191.96.234.0 - 191.96.237.255
191.96.239.0 - 191.96.239.255
191.96.244.0 - 191.96.244.255
191.96.246.0 - 191.96.246.255
191.101.25.0 - 191.101.25.255
191.101.36.0 - 191.101.39.255
191.101.40.0 - 191.101.47.255
191.101.128.0 - 191.101.134.255
191.101.146.0 - 191.101.147.255
191.101.148.0 - 191.101.149.255
191.101.176.0 - 191.101.177.255
191.101.182.0 - 191.101.182.255
191.101.184.0 - 191.101.189.255
191.101.192.0 - 191.101.197.255
191.101.204.0 - 191.101.207.255
191.101.216.0 - 191.101.220.255
191.101.222.0 - 191.101.223.255
196.62.0.0 - 196.62.255.255
204.52.96.0 - 204.52.117.255
204.52.120.0 - 204.52.121.255
204.52.122.0 - 204.52.122.255
204.52.124.0 - 204.52.127.255
206.124.104.0 - 206.124.111.255
209.192.128.0 - 209.192.159.255

216.173.64.0 - 216.173.127.255

ATTACHMENT B

Particular Things To Be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the period from January 1, 2015 to January 1, 2017:

a. All records and other information pertaining to the Target IPs, including all files, databases, IP logs and database records stored by the Provider in relation to the Target IPs;

b. All information in the possession of the Provider that might identify the subscriber(s) and user(s) related to the Target IPs, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service utilized by the subscriber(s) and user(s) of the Target IPs;

d. All records pertaining to communications between the Provider and any person regarding the Target IPs, including contacts with support services and records of actions taken;

e. All records pertaining to the physical location of the servers used to host the Target IPs;

f. All files, databases and other content information pertaining to the Target IPs stored on behalf of its subscriber(s) and user(s), including:

1. All volatile memory used by virtualized and physical computers;
2. Programming code used to serve or process requests from email clients;
3. SSH, FTP or similar logs showing connections related to the Target IPs, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;
4. MySQL, PostgreSQL, or other databases related to website(s);
5. Email accounts and the contents thereof, associated with the servers; and
6. A forensic image of the servers associated with the Target IPs, including any historic images;

g. All records and information, including passwords, encryption keys, and other access devices, that may be necessary to access the information associated with the Target IPs.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and wire fraud conspiracy), those violations involving the user(s) of the servers associated with the Target IPs, their co - conspirators, their associates and others with whom they communicated, including information pertaining to the following matters:

a. Committing, conspiring or attempting to commit wire fraud;

b. Evidence indicating how and when the servers associated with the Target IPs were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the servers' users;

c. Evidence indicating the state of mind of the user(s) of the servers associated with the Target IPs, as it relates to the crimes under investigation;

d. The identity of the person(s) who leased, used, or controlled the servers associated with the Target IPs, including records that help reveal the whereabouts of such person(s).

e. The identity of the persons(s) and computer(s) that communicated with the servers associated with the Target IPs in relation to wire fraud and conspiracy or attempt to commit wire fraud, including records that help reveal their whereabouts.